SIAM J. DISCRETE MATH.
Vol. 23, No. 1, pp. 59–78

ON COSETS OF WEIGHT 4 OF $BCH(2^m, 8)$, m EVEN, AND EXPONENTIAL SUMS*

PASCALE CHARPIN†, TOR HELLESETH‡, AND VICTOR ZINOVIEV§

Abstract. We give exact expressions for the number of coset leaders in the cosets of weight 4 of binary primitive narrow sense Bose–Chaudury–Hocquenghem (BCH) codes of length $n = 2^m$ (m even) with minimum distance 8 in terms of several exponential sums, including cubic sums and Kloosterman sums. This allows us to bound the number of coset leaders in these cosets.

Key words. binary primitive narrow sense BCH code, coset, coset weight distribution, exponential sum, cubic sum, Kloosterman sum, partial sum, inverse cubic sum

AMS subject classifications. 11T71, 11T23

DOI. 10.1137/070692649

1. Introduction. This paper is a natural continuation of our previous papers [3], [4], [5], and [6]. In these papers, we studied the coset weight distributions of binary extended triple-error-correcting primitive narrow sense Bose–Chaudury–Hocquenghem (BCH) codes. Such a code is of length 2^m and minimum distance 8, which we will denote by $BCH(2^m, 8)$, and is the extension of the binary cyclic code of length $2^m - 1$ and designed distance 7, i.e., the cyclic code with zeros set $\{\alpha,\ \alpha^3,\ \alpha^5\}$ (where α is a primitive root of the finite field of order 2^m).

In [3] and [4] we described coset weight distributions of $BCH(2^m, 8)$ for odd m for the cosets of any weight $j = 1, 2, 3, 4, 5, 6$. For the cosets of weight 4, using an approach developed in [11], we have found [4] the exact expressions for the number of words of weight 4 in terms of the exponential sums of four different types, in particular, of the Kloosterman sums over $GF(2^m)$. Using these results we obtained new properties of Kloosterman sums, mainly their divisibility modulo 24 (see [5]).

The purpose of this paper is to obtain similar results in the case where m is even. Here we extend these results for even m, obtaining explicit expressions for the number of words of weight 4 of cosets of weight 4 of $BCH(2^m, 8)$. For the codes $BCH(2^m, 8)$ the case of even m is much harder, since the exact expressions depend on five different exponential sums. Analyzing these sums we reduce the final expressions to the exponential sums of four different types, including cubic sums and Kloosterman sums. Known bounds for values of these sums permit us to bound the number of words of weight 4 in the cosets of weight 4.

This paper is organized as follows. In section 2, following [3] and [10] we give some preliminary results concerning the codes $BCH(2^m, 8)$ and exponential sums over $GF(2^m)$, in particular, the cubic sums and Kloosterman sums. In section 3 we consider a nonlinear system of equations, which defines the number of words of weight

*Received by the editors May 22, 2007; accepted for publication (in revised form) June 16, 2008; published electronically October 24, 2008. This work was supported by INRIA-Rocquencourt, by the Norwegian Research Council under grant 171094/V30, and also by the Russian Fund of Fundamental Researches (project 06-01-00226).

http://www.siam.org/journals/sidma/23-1/69264.html

†INRIA, Domaine de Voluceau-Rocquencourt, BP 105-78153, Le Chesnay, France (pascale.charpin@inria.fr).

‡Department of Informatics, University of Bergen, N-5020 Bergen, Norway (torh@ii.uib.no).

§Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia (zinov@iitp.ru).

4 in a coset of weight 4 of a code $BCH(2^m, 8)$. In section 4 we solve the nonlinear system of equations, which gives the number of words of weight 4 for any such coset. We express the number of solutions to this system in terms of the exponential sums of four different types: the two cubic sums, the Kloosterman sums, and the so-called inverse cubic sum. Here we use the same approach as in [10], [11], [12]. Using known results on exponential sums, we lower and upper bound the number of words of weight 4 in any coset of weight 4. In section 5 we compute all of the possible values of the number of words for the first nontrivial values $m = 6$ and $m = 8$.

2. Definitions and preliminary results. The Hamming *weight* of any vector (or word) x is denoted by $wt(x)$. Generally, we denote by $\mathbf{F}_{2^k}$ the finite field of order 2^k. However, we simply denote by $\mathbf{F}$ the field $\mathbf{F}_{2^m}$. For any set E containing 0 we denote: $E^* = E \setminus \{0\}$. Also, $\#E$ denotes the cardinality of any set E.

Let us denote by $BCH(2^m, 8)$ a binary primitive (in narrow sense) extended BCH code of length $n = 2^m$, where $m \geq 5$, and the minimal distance is 8. This is the code over $GF(2)$ with the parity check matrix given by

$$H_B \;=\; \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-2} \\ 0 & 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{(n-2)3} \\ 0 & 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{(n-2)5} \end{bmatrix},$$

where α is a primitive root of $\mathbf{F}$ (see [16, ch. 7, section 6]). We use the elements of $\mathbf{F}$ as locators for the code $BCH(2^m, 8)$, where the first position of $BCH(2^m, 8)$ corresponds to the zero element of $\mathbf{F}$.

Let $D = x + BCH(2^m, 8)$ be a coset of $BCH(2^m, 8)$. *The weight of the coset* D is the minimum weight of the words of D. *A leader* of D is a codeword of D of minimum weight. To this coset D we associate a *syndrome*, which is a vector, say S, over $\mathbf{F}$ with four coordinates:

$$S \;=\; (S_1, S_2, S_3, S_4) \;=\; xH_B^t,$$

where x is any vector from D and H_B^t is the transpose of the matrix H_B. In this paper we consider only cosets D of weight four. Since the first component S_1 of the syndrome S shows the parity of the vector x, in the rest of this paper, under a syndrome of a coset D, we use the vector (S_2, S_3, S_4), i.e., without the first (zero) coordinate. Recall that the covering radius of $BCH(2^m, 8)$ is 6 [9]. Therefore, the weight i of D is in the set $\{0, \ldots, 6\}$.

Let $Tr(x)$ denote the absolute trace of $x \in \mathbf{F}$ and, for even m, denote by $x \mapsto Tr_2^m(x)$ the trace function from $\mathbf{F}$ to its subfield $\mathbf{F}_4$.

LEMMA 1 (see [11]). *Let a, b be two arbitrary elements of $\mathbf{F}^*$, $a \neq b$. Then*

$$Tr\left(\frac{a\,b}{(a+b)^2}\right) \;=\; 0.$$

LEMMA 2 (see [15]). *The quadratic equation $x^2 + ax + b = 0$, $a \in \mathbf{F}^*, b \in \mathbf{F}$, has two different roots in $\mathbf{F}$ if $Tr(b/a^2) = 0$ and no roots in $\mathbf{F}$ if $Tr(b/a^2) = 1$.*

LEMMA 3 (see [1]). *The cubic equation $x^3 + ax + b = 0$, where $a \in \mathbf{F}$ and $b \in \mathbf{F}^* = \mathbf{F} \setminus \{0\}$, has a unique solution in $\mathbf{F}$ if and only if $Tr(a^3/b^2) \neq Tr(1)$. Furthermore, if it has three distinct roots in $\mathbf{F}$, then $Tr(a^3/b^2) = Tr(1)$.*

Denote $f_b(x) = x^3 + x + b$, where $b \in \mathbf{F}^*$. Let

$$M_i = \#\{\ b\ :\ f_b(x) \text{ has precisely } i \text{ zeros in } \mathbf{F}\ \}.$$

LEMMA 4 (see [13]). *Let $n = 2^m$ where m is even. Then clearly $M_2 = 0$ and*

$$\begin{aligned} M_0 &= (n-1)/3, \\ M_1 &= n/2, \\ M_3 &= (n-4)/6. \end{aligned}$$

Denote

$$e(a) \ = \ (-1)^{Tr(a)}.$$

The function $e(x)$ is an additive character of $\mathbf{F}$. For any mapping $f : \mathbf{F} \mapsto \mathbf{F}$, the expression of the type

$$\sum_{x \in \mathbf{F}} e(f(x))$$

is called an exponential (or a character) sum over $\mathbf{F}$.

LEMMA 5 (see [4]). *Let σ be any mapping from $\mathbf{F}$ to $\mathbf{F}$, and let $\lambda \in \mathbf{F}^*$. Denote by H the kernel of the linear function $x \mapsto Tr(\lambda x)$. Then*

$$\sum_{x \in F} e(\sigma(x)) + \sum_{x \in F} e(\sigma(x) + \lambda x) = 2 \sum_{x \in H} e(\sigma(x)).$$

The exponential sums of polynomials of degree three over $\mathbf{F}$ are known; they are known also from coding theory (see [16, chapter 15]). In particular, we need the following result due to Carlitz [2]. For arbitrary elements $a \in \mathbf{F}^*$ and $b \in \mathbf{F}$, denote

$$C(a,\, b) \ = \ \sum_{x \in \mathbf{F}} e(a\, x^3 \ + \ b\, x), \quad C(a) \ = \ C(a, 0).$$

LEMMA 6 (see [2]). *Let $a \in \mathbf{F}^*$. For any even $m = 2s$ we have that*

$$C(a) \ = \ \begin{cases} (-1)^{s+1} 2^{s+1} & \text{if } a \text{ is a cube in } \mathbf{F}, \\ (-1)^s 2^s & \text{otherwise.} \end{cases}$$

If $a = \beta^3, \ \ \beta \in \mathbf{F}$, then

$$C(a,b) \ = \ \begin{cases} (-1)^{s+1} 2^{s+1} e(x_0^3) & \text{if } Tr_2^m(b\beta^{-1}) = 0, \\ 0 & \text{otherwise,} \end{cases}$$

where x_0 denotes any solution of $x^4 + x = \beta^{-2} b^2$.

If $a \neq \beta^3, \ \ \beta \in \mathbf{F}$, then

$$C(a,b) \ = \ (-1)^s 2^s\, e(a\, x_1^3),$$

where x_1 is the unique solution of $a^2 x^4 + a\, x \ = \ b^2$, given by

$$\left(a^{(2^{2s}-1)/3} + 1\right)\, x_1 \ = \ \sum_{j=0}^{s-1} \left(a^{-1} b^2\right)^{2^{2j}}\ a^{(2^{2j}-1)/3}.$$

We also need the exponential sums of such type for the case when the argument x runs over $\mathbf{F}$ with the fixed trace of the element $1/x$. It is convenient for us to define this partial sum multiplied by 2:

$$P(a,\, b) \;=\; 2 \sum_{x\in\mathbf{F}:\; Tr(1/x)=0} e(a\,x^3 \;+\; b\,x). \tag{2.1}$$

Recall that the classical binary Kloosterman sum, say $K'(a)$, is defined for each a in $\mathbf{F}^*$ by

$$K'(a) \;=\; \sum_{x\in\mathbf{F}^*} e\left(a\,x \;+\; \frac{1}{x}\right).$$

The exponential sums, which we consider here, are generally defined on $\mathbf{F}^*$, the multiplicative group of $\mathbf{F}$. In this paper we extend all of the sums to 0, assuming that $e(x^{-1}) = e(x^{-3}) = 1$ for $x = 0$. Indeed, $Tr(x^{-1}) = Tr(x^{2^{m-1}-1})$ so that we can define $Tr(x^{-1}) = 0$ for the case $x = 0$. Therefore, we define here the classical Kloosterman sum $K(a),\ a \in \mathbf{F}^*$, as

$$K(a) \;=\; \sum_{x\in\mathbf{F}} e\left(a\,x \;+\; \frac{1}{x}\right) \;=\; K'(a) \;+\; 1. \tag{2.2}$$

We extend the sum $K'(a)$ to $a = 0$, setting $K(0) \;=\; 0$.

Note that we have (where $x = ya$ and $z^2 = y$)

$$\sum_{x\in\mathbf{F}} e\left(\frac{a}{x} + ax\right) = \sum_{y\in\mathbf{F}} e\left(\frac{1}{y} + a^2 y\right) = \sum_{z\in\mathbf{F}} e\left(\frac{1}{z} + az\right) = K(a). \tag{2.3}$$

And obviously $K(a) \;=\; K(a^2)$.

Using deep results on the number of rational points on certain elliptic curves, Lachaud and Wolfmann [14] proved the following result.

LEMMA 7. *The set $K(a),\ a \in \mathbf{F}$ is the set of all the integers $s \equiv\ 0 \pmod 4$ with value s in the range $[-2^{(m/2)+1} + 1,\ 2^{(m/2)+1} + 1]$.*

Note that we deduce immediately that for m even and for any $a \in \mathbf{F}$, we have

$$-2^{(m/2)+1} + 4 \le K(a) \le 2^{(m/2)+1}. \tag{2.4}$$

Considering the coset weight distribution of Z_4-linear Goethals codes, we obtained the following result.

LEMMA 8 (see [10]). *For any $m \ge 3$,*

$$K(a) \;\equiv\; \begin{cases} 4 \mod 8 & if \quad Tr(a) = 1, \\ 0 \mod 8 & if \quad Tr(a) = 0. \end{cases}$$

We also need the following observation, partly given in [4].

LEMMA 9. *For any $a \in \mathbf{F}^*$ and for any m,*

$$K(a) = 2 \sum_{x\in\mathbf{F}:\; Tr(1/x)=0} e(ax) = -\,2 \sum_{x\in\mathbf{F}:\; Tr(1/x)=1} e(ax).$$

Proof. We first have

$$K(a) = \sum_{x,\; Tr(1/x)=0} e(ax) - \sum_{x,\; Tr(1/x)=1} e(ax).$$

Since

$$\sum_{x\in\mathbf{F}} e(ax) = 0 = \sum_{x,\ Tr(1/x)=0} e(ax) + \sum_{x,\ Tr(1/x)=1} e(ax),$$

we obtain the equality of the lemma using

$$\sum_{x,\ Tr(1/x)=0} e(ax) = -\sum_{x,\ Tr(1/x)=1} e(ax). \qquad \square$$

We also need the following sum $G'(a,b)$, which we introduced in [4], and which we call an *inverse cubic*:

$$G'(a,b) \ = \ \sum_{x\in\mathbf{F}^*} e\left(a\,x^3 \ + \ \frac{b}{x}\right), \quad a\in\mathbf{F}^*,\ b\in\mathbf{F}.$$

Here we also extend this sum to $x=0$, setting $bx^{-1}=0$ at the point $x=0$. Thus

$$G(a,b) \ = \ \sum_{x\in\mathbf{F}} e\left(a\,x^3 \ + \ \frac{b}{x}\right) \ = \ G'(a,b) \ + \ 1.$$

It is easy to check that $G(a,a) = G(a^2,a^2)$. This follows immediately from the equality $G'(a,a) = G'(a^2,a^2)$, which was given in [4]. We also have to bound these sums.

LEMMA 10. *Let m be even. For any $a,b\in\mathbf{F}$, where $(a,b)\neq(0,0)$, we have*

$$|G(a,b)| \le 2^{m/2+2}. \tag{2.5}$$

Proof. We gave an upper bound on $|G'(a,b)|$ in [4, Lemma 14] for odd m, but it is easy to check that our proof in [4] holds for even m too. This upper bound is as follows:

$$|G'(a,b)| \ \le \ 4\sqrt{2^m}.$$

Since $G(a,b)$ is a multiple of 4 for any $a,b\in\mathbf{F}$ and $G(a,b)=G'(a,b)+1$, the proof is completed. $\square$

Now, by the two next lemmas, we introduce some important relations linking partial sums with other sums considered here. To see the difference between even and odd cases, we formulate these results for both m, even and odd, and prove only the even cases. The odd cases are, respectively, Lemmas 10 and 12 in [4]. We mention that the partial sum $P(a,b)$, defined in [4], is not doubled (as here).

LEMMA 11. *Let a be any element of $\mathbf{F}^*$, where $\mathbf{F}$ has the order 2^m. Then*

$$P(a,a) \ = \ \begin{cases} K(a) \ + \ 2\,C(a,a) & if\ m\ is\ even, \\ K(a) & if\ m\ is\ odd. \end{cases}$$

Proof. Let m be even. We first have

$$\sum_{x\in\mathbf{F}} e(a(x^3+x)) = \sum_{x\in\mathbf{F},\ Tr(1/x)=0} e(a(x^3+x)) + \sum_{x\in\mathbf{F},\ Tr(1/x)=1} e(a(x^3+x))$$

which means

$$C(a,a) \ = \ \frac{1}{2}\,P(a,a) + \sum_{x\in\mathbf{F},\ Tr(1/x)=1} e(a(x^3+x)). \tag{2.6}$$

Moreover, in the case where m is even,

$$\{\ x^3+x \mid x\in\mathbf{F},\ Tr(1/x)=1\ \} = \{\ y\in\mathbf{F} \mid Tr(1/y)=1\ \}. \tag{2.7}$$

This is because

$$Tr\left(\frac{1}{x^3+x}\right) = Tr\left(\frac{1}{x}+\frac{1}{x+1}+\frac{1}{x^2+1}\right),$$

and the equation $x^3+x+c=0$ has a unique solution if and only if $Tr(1/c)=1$. We know that there are $M_1=2^{m-1}$ such c and then 2^{m-1} elements x^3+x (in the set above on the right) since for every such c

$$Tr\left(\frac{1}{c}\right) = Tr\left(\frac{1}{x^3+x}\right) = Tr\left(\frac{1}{x}\right) = 1$$

(see Lemmas 3 and 4). So, both sets in (2.7) have the same cardinality M_1. We deduce

$$\sum_{x\in\mathbf{F},\ Tr(1/x)=1} e(a(x^3+x)) = \sum_{y\in\mathbf{F},\ Tr(1/y)=1} e(ay).$$

Using (2.6) and Lemma 9, we get

$$P(a,a) \ = \ 2\,C(a,a) \ - \ 2\sum_{y\in\mathbf{F},\ Tr(1/y)=1} e(ay) \ = \ 2\,C(a,a) \ + \ K(a). \qquad \square$$

LEMMA 12. *For any $a\in\mathbf{F}^*$,*

$$P(a,0) \ = \ \begin{cases} G(a,a) \ + \ C(a) & if\ m\ is\ even,\\ G(a,a) & if\ m\ is\ odd. \end{cases}$$

Proof. Recall that we denote $C(a)=C(a,0)$. Also

$$P(a,0) = 2\sum_{x,\ Tr(1/x)=0} e(ax^3).$$

We have, using Lemma 5,

$$\sum_{x\in\mathbf{F}} e(ax^{-3}) + \sum_{x\in\mathbf{F}} e(ax^{-3}+x) = 2\sum_{x,\ Tr(x)=0} e(ax^{-3}) = P(a,0),$$

with

$$\sum_{x\in\mathbf{F}} e(ax^{-3}) = \sum_{x\in\mathbf{F}} e(ax^3) = C(a)$$

and, moreover,

$$\begin{aligned} G(a,1) &= \sum_{x\in\mathbf{F}} e(ax^3+x^{-1}) = \sum_{y\in\mathbf{F}} e(a^4y^3+y^{-1})\\ &= \sum_{z\in\mathbf{F}} e(az^3+az^{-1}) \ = \ G(a,a), \end{aligned}$$

with $y=x^4$ and $z=ay$. $\square$

3. Cosets of weight four in terms of nonlinear systems of equations. Let D be a coset of $BCH(2^m, 8)$ with syndrome $S = (a, b, c)$. To find the number of coset leaders in D, one needs to solve the following system of equations over $\mathbf{F}$:

$$\begin{aligned} x \;+\; y \;+\; z \;+\; u &= a, \\ x^3 \;+\; y^3 \;+\; z^3 \;+\; u^3 &= b, \\ x^5 \;+\; y^5 \;+\; z^5 \;+\; u^5 &= c. \end{aligned} \tag{3.1}$$

Here x, y, z, and u are pairwise distinct elements of $\mathbf{F}$. Here we are interested in cosets of weight 4 which are not contained in the Reed–Muller code of order $m-2$. That is, $\{x, y, z, u\}$ is not a 2-dimensional flat or, equivalently, $a \neq 0$ in (3.1). For the case of odd m, cosets which are contained in the Reed–Muller code of order $m-2$ have been described in [3]. The approach, which we used in [3] for odd m, can be used, of course, for the case of even m.

Denote by $\mu(a, b, c)$ the number of different solutions to the system (3.1), i.e., the number of unordered 4-sets of different elements x, y, z, u of $\mathbf{F}$, which satisfy (3.1). So, for fixed elements $a, b, c \in \mathbf{F}$, this number defines exactly the number of leaders of D.

We now recall some general properties of our system (3.1). They can be checked easily and have been considered for odd m in more detail but with another terminology in [3, Lemma 4.4].

PROPOSITION 1. *A 4-tuple $\{x, y, z, u\}$ is a solution to* (3.1) *for given (a, b, c) if and only if a 4-tuple $\{g\,x, g\,y, g\,z, g\,u\}$ is a solution to* (3.1) *for given (a', b', c'), where*

$$a' = g\,a, \qquad b' = g^3 b, \qquad c' = g^5 c, \qquad g \in \mathbf{F}^*.$$

PROPOSITION 2. *A 4-tuple $\{x, y, z, u\}$ is a solution to* (3.1) *for given (a, b, c) if and only if a 4-tuple $\{x+h, y+h, z+h, u+h\}$, $h \in \mathbf{F}$, is a solution to* (3.1) *for given (a', b', c'), where*

$$a' = a, \qquad b' = b + ha(h + a), \qquad c' = c + ha(h^3 + a^3).$$

PROPOSITION 3. *A 4-tuple $\{x, y, z, u\}$ is a solution to* (3.1) *for given (a, b, c) if and only if a 4-tuple $\{x^2, y^2, z^2, u^2\}$ is a solution to* (3.1) *for given (a', b', c'), where*

$$a' = a^2, \qquad b' = b^2, \qquad c' = c^2.$$

For fixed a, b, and c, denote by $V(a, b, c)$ the set of all 4-sets $\{x, y, z, u\}$ which are solutions to (3.1), i.e., in our notation $\#V(a, b, c) = \mu(a, b, c)$. Denote by $\mathcal{V}$ all of the sets of 4-sets, which are solutions to (3.1) for some a, b, c,

$$\mathcal{V} = \bigcup_{a \in \mathbf{F}^*,\ b, c \in \mathbf{F}} V(a, b, c).$$

This set $\mathcal{V}$ can be partitioned into different orbits, which are induced by applying Propositions 1–3.

DEFINITION 1. *For given elements $a, b, c \in \mathbf{F}$ we define the orbit $\mathcal{O}(a, b, c)$ as the set of $V(a', b', c')$, which can be obtained from $V(a, b, c)$ by all possible transformations given in Propositions* 1–3.

According to Propositions 1–3, all sets $V(a', b', c')$ from the orbit $\mathcal{O}(a, b, c)$ have the same cardinality $\mu(a, b, c)$. For arbitrary element $\eta \in \mathbf{F}$, we denote by $\ell_{\eta, m}$ the size

of the cyclotomic coset $C_\eta = \{\eta, \eta^2, \eta^{2^2}, \ldots\}$ of η induced by the action of Frobenius automorphisms of $\mathbf{F} = GF(2^m)$, i.e.,

$$\ell_{\eta,m} = \#C_\eta = \min\{s \mid s > 0,\ \eta^{2^s} = \eta\}.$$

Now we are going to prove that all orbits $\mathcal{O}(a,b,c)$ have a cardinality which depends on the value of $\ell_{\eta,m}$ only, for some η which is defined by the next lemma.

LEMMA 13. *Let a, b, c be arbitrary elements of $\mathbf{F}$, where $a \neq 0$. Let $\mu(a,b,c)$ be the number of solutions to the system* (3.1).

(i) *If $Tr(b/a^3) = 0$, then*

$$\mu(a,b,c) = \mu(1,0,\eta),$$

where

$$\eta = \frac{c}{a^5} + \frac{b^2}{a^6} + \frac{b}{a^3}. \tag{3.2}$$

(ii) *If $Tr(b/a^3) = 1$, then*

$$\mu(a,b,c) = \mu(1,\delta,\eta),$$

where δ is an arbitrary element of $\mathbf{F}^*$ with $Tr(\delta) = 1$ and where

$$\eta = \frac{c}{a^5} + \frac{b^2}{a^6} + \frac{b}{a^3} + \delta^2 + \delta.$$

Proof. Consider an arbitrary set $V(a,b,c)$, where a, b, c are arbitrary elements of $\mathbf{F}$ and $a \neq 0$. Using Proposition 1 with $g = 1/a$, we obtain the set $V(1, b/a^3, c/a^5)$, which has the same cardinality as $V(a,b,c)$. Now we apply Proposition 2 to this set. We obtain for any h,

$$V(1,\ b/a^3 + h(h+1),\ c/a^5 + h(h^3+1)).$$

First, assume that $Tr(b/a^3) = 0$. Consider the following quadratic equation on h:

$$h^2 + h + \frac{b}{a^3} \ = \ 0. \tag{3.3}$$

Since $Tr(b/a^3) = 0$, this equation has two distinct roots h_1 and h_2 in the field $\mathbf{F}$, and we choose any one of these roots as h. In such a way we obtain the set $V(1,0,\eta)$ where

$$\eta \ = \ \frac{c}{a^5} \ + \ h^4 \ + \ h. \tag{3.4}$$

Summing expression (3.3) and the expression obtained by squaring of (3.3), we arrive at the following formula for $h^4 + h$:

$$h^4 \ + \ h \ = \ \frac{b}{a^3} \ + \ \frac{b^2}{a^6},$$

which does not depend on the choice of the roots h_1 and h_2. Using this equality in (3.4), we obtain the formula (3.2) for η, given in Lemma 13 for the case (i).

Now consider the case (ii), when $Tr(b/a^3) = 1$. In this case (3.3) has no solutions in $\mathbf{F}$. Hence we cannot eliminate the element b/a^3, or even reduce it to 1. In this

case we cannot do anything better than choose $\delta \in F^*$ such that $Tr(\delta) = 1$, with h satisfying

$$h^2 + h + \frac{b}{a^3} + \delta = 0.$$

For any such element δ the equation above has two solutions, say h_1 and h_2. Hence, for a given b/a^3, we can take any element δ with $Tr(\delta) = 1$. Then we get the set $V(1, \delta, \eta)$, which has the same cardinality as $V(a, b, c)$. The expression for η is obtained in the same way as for η above. □

Note that for any i the set $V(1, 0, \eta^{2^i})$ belongs to the orbit $\mathcal{O}(1, 0, \eta)$, by definition of the orbits. Also, we have

$$V(1, \delta^{2^i}, \eta^{2^i}) \in \mathcal{O}(1, \delta, \eta).$$

Thus, according to Lemma 13, the set $\mathcal{V}$ is partitioned into the orbits of two types: $\mathcal{O}(1, 0, \eta)$ and $\mathcal{O}(1, \delta, \eta)$. We are going to compute the cardinality of these orbits. Our next proposition, together with Lemma 13, gives the length of any orbit $\mathcal{O}(a, b, c)$.

PROPOSITION 4. *The parameters η and δ are defined by Lemma* 13. *The length of the orbit $\mathcal{O}(1, 0, \eta)$ and the length of the orbit $\mathcal{O}(1, \delta, \eta)$ only depend on the size $\ell_{\eta,m}$ of the cyclotomic coset C_η of η. More precisely,*

$$\#\mathcal{O}(1, 0, \eta) = \#\mathcal{O}(1, \delta, \eta) = (2^m - 1)2^{m-1}\ell_{\eta,m}.$$

Proof. First, note that by Lemma 13 we proved that for any (a, b, c), the set $V(a, b, c)$ is either in $\mathcal{O}(1, 0, \eta)$ or $\mathcal{O}(1, \delta, \eta)$, for some δ such that $Tr(\delta) = 1$, where η is uniquely defined.

Let η be any element of $\mathbf{F}$. According to Definition 1, we have to count the number of distinct sets $V(a, b, c)$ which belong to $\mathcal{O}(1, 0, \eta)$. We can choose in 2^{m-1} ways an element $\beta \in \mathbf{F}$ and, further, the element $a \in \mathbf{F}^*$ in $2^m - 1$ ways. To be clear, we proceed as follows:

$$(1, 0, \eta) \longrightarrow (1, \beta = h^2 + h, \eta + h^4 + h) \longrightarrow (a, \beta a^3, (\eta + \beta + \beta^2)a^5)$$

and obtain $(2^m - 1)2^{m-1}$ different triples

$$(a, b, c), \quad b = \beta a^3, \quad \text{and} \quad c = (\eta + \beta + \beta^2)a^5.$$

Moreover, for each such triple, the sets $V(a, b, c_i)$ with $c_i = (\eta^{2^i} + \beta + \beta^2)a^5$ also belong to $\mathcal{O}(1, 0, \eta)$, which allow us to get at all $(2^m - 1)2^{m-1}\ell_{\eta,m}$ elements.

We proceed in the same way to count the number of distinct sets $V(a, b, c)$ which belong to $\mathcal{O}(1, \delta, \eta)$ (where $Tr(\delta) = 1$). We have, as before

$$(1, \delta, \eta) \rightarrow (1, \beta = \delta + h^2 + h, \eta + h^4 + h) \rightarrow (a, \beta a^3, (\eta + \beta + \delta + (\beta + \delta)^2)a^5)$$

and then $(2^m - 1)2^{m-1}$ different triples

$$(a, b, c), \quad b = \beta a^3, \quad \text{and} \quad c = (\eta + \beta + \delta + (\beta + \delta)^2)a^5.$$

Note that the image of the map $h \mapsto h + h^2 + \delta$ is the set of all β such that $Tr(\beta) = 1$. This image does not depend on δ. We have to take into account that $V(1, \delta^{2^i}, \eta^{2^i})$ belongs to $\mathcal{O}(1, \delta, \eta)$ for any i. Due to our previous remark, we have to consider only the length of C_η, providing that the cardinality of $\mathcal{O}(1, \delta, \eta)$ equals $(2^m - 1)2^{m-1}\ell_{\eta,m}$. □

Remark 1. In this section, we assume that $a \neq 0$ for the study of $\mu(a,b,c)$. When $a = 0$ then the corresponding coset, say D, is contained in the Reed–Muller code of order $m-2$. According to Proposition 3, it is clear that *if* $\{x,y,z,u\}$ *is a solution to* (3.1) *for given* $(0,b,c)$*, then any* 4*-tuple* $\{x+h, y+h, z+h, u+h\}$ *is a solution too, for any* $h \in \mathbf{F}$. In this case the coset D is such that each coordinate position is covered by at least one leader of D. Since the weight of D is 4, the supports of two leaders cannot intersect, proving that the number of leaders is 2^{m-2}. Since any leader of D is a minimum codeword of the Reed–Muller code of order $m-2$, its support is an affine subspace of dimension 2. As there are $(2^m-1)(2^m-2)/6$ linear subspaces of dimension 2, there are also the same number of cosets of B of weight 4 corresponding to triples of the form $(0,b,c)$.

4. On the number of solutions to the system of equations and exponential sums. The main result of this paper is the following explicit expression for the number of solutions to the system (3.1) in terms of four different types of exponential sums. We repeat the corresponding result from [4] for odd m and a new result for even m as one theorem (for completeness and to see the difference between these two cases).

THEOREM 1. *Let* $\mu(a,b,c)$ *be the number of different* 4*-sets* $\{x,y,z,u\}$*, where* x,y,z,u *are pairwise distinct elements of* $\mathbf{F}$*, which are solutions to the system* (3.1)*, where* $a,b,$ *and* c *are arbitrary elements of a field* $\mathbf{F}$ *of cardinality* 2^m $(m \geq 4)$ *and* $a \neq 0$*. Let*

$$\epsilon = Tr\left(\frac{b}{a^3}\right) \quad \textit{and} \quad \lambda = \frac{b}{a^3}\left(\frac{b}{a^3}+1\right) + \frac{c}{a^5} + 1. \tag{4.1}$$

If $\lambda \neq 0$*, then*

$$\mu(a,b,c) \;=\; \mu(\epsilon,\lambda) \;=\; \frac{1}{3}\,M(\epsilon,\lambda) \tag{4.2}$$

where $M(\epsilon,\lambda)$ *is even and equal to: for even* m

$$\begin{aligned} 8\,M(\epsilon,\lambda) &= 2^m \;-\; 8 \;+\; 3G(\lambda,\lambda) \;+\; C(\lambda) \\ &\quad + (-1)^{\epsilon}\,(2K(\lambda) \;+\; 4C(\lambda,\lambda) \;-\; 8)\,, \end{aligned} \tag{4.3}$$

and for odd m

$$\begin{aligned} 8\,M(\epsilon,\lambda) &= 2^m \;-\; 8 \;+\; 3G(\lambda,\lambda) \\ &\quad + (-1)^{\epsilon+1}\,(2K(\lambda) \;+\; 2C(\lambda,\lambda) \;-\; 8)\,. \end{aligned} \tag{4.4}$$

If $\lambda = 0$*, then*

$$\mu(\epsilon,0) \;=\; 0.$$

We want to solve the system (3.1) for the general case $Tr(b/a^3) = \epsilon$. Thus, we do not use the reduced form $\mathcal{O}(1,0,\eta)$ or $\mathcal{O}(1,\delta,\eta)$ of the orbits of solutions $\mathcal{O}(a,b,c)$, obtained in the previous section. For our purposes we consider the system (3.1) in the following form:

$$\begin{aligned} x \;+\; y \;+\; z \;+\; u &= 1, \\ x^3 \;+\; y^3 \;+\; z^3 \;+\; u^3 &= b', \\ x^5 \;+\; y^5 \;+\; z^5 \;+\; u^5 &= c', \end{aligned} \tag{4.5}$$

where x, y, z, and u are pairwise distinct elements of $\mathbf{F}$ and where $b' = b/a^3$ and $c' = c/a^5$ are arbitrary elements of $\mathbf{F}$. From now on, we use the following notation:

$$\mathbf{F}^{**} = \mathbf{F} \setminus \{0, 1\}.$$

Before we begin to prove the theorem we give one simple lemma and several statements, which reduce some exponential sums to the sums, which we introduced in section 2.

LEMMA 14. *Let* $\{x, y, z, u\}$ *be a solution to* (4.5). *Then a* 4*-set* $\{x+1, y+1, z+1, u+1\}$ *is a solution to* (4.5).

Proof. The proof follows by direct checking. ∎

Define three following functions $g_i(v)$ from $\mathbf{F}^{**}$ to $\mathbf{F}^{**}$:

$$\begin{aligned} g_1(v) &= \lambda\left(\frac{v+1}{v^3}\right), \\ g_2(v) &= \lambda\left(\frac{v}{(v+1)^3}\right), \\ g_3(v) &= \lambda\left(\frac{1}{v} + \frac{1}{v+1}\right). \end{aligned}$$

Denote by $S(g)$ the following exponential sum:

$$S(g) = \sum_{v \in \mathbf{F}^{**}} e(g(v)).$$

PROPOSITION 5. *Let* $\lambda \neq 0$. *Then*

$$S(g_1) = S(g_2) = C(\lambda, \lambda) - 2.$$

Proof. Since $g_1(v) = g_2(v+1)$, we have that $S(g_1) = S(g_2)$. Consider $S(g_1)$:

$$\begin{aligned} S(g_1) &= \sum_{v \in \mathbf{F}^{**}} e\left(\lambda \frac{v+1}{v^3}\right) \\ &= \sum_{v \in \mathbf{F}^{**}} e\left(\frac{\lambda}{v^2} + \frac{\lambda}{v^3}\right) \\ &= \sum_{\xi \in \mathbf{F}^{**}} e(\lambda(\xi^3 + \xi^2)) \\ &= \sum_{\zeta \in \mathbf{F}^{**}} e(\lambda(\zeta^3 + \zeta)) \\ &= C(\lambda, \lambda) - 2, \end{aligned}$$

where we twice changed the variable $v = 1/\xi$ and $\xi = \zeta + 1$. ∎

PROPOSITION 6. *Let* $\lambda \neq 0$. *Then*

$$S(g_3) = K(\lambda) - 2.$$

Proof. This result is an instance of [7, Theorem 1]. We briefly give the proof for

clarity and completeness:

$$\begin{aligned} S(g_3) &= \sum_{v\in\mathbf{F}^{**}} e\left(\frac{\lambda}{v}+\frac{\lambda}{v+1}\right) \\ &= \sum_{h\in\mathbf{F}^{**}} e\left(\frac{\lambda h^2}{h+1}\right) \\ &= \sum_{h\in\mathbf{F}^{**}} e\left(\lambda\,(h+1)+\frac{\lambda}{h+1}\right) \\ &= K(\lambda) \;-\; 2, \end{aligned}$$

where $h = 1/v$ and using (2.3). ∎

PROPOSITION 7. *Let $\lambda \neq 0$. Then*

$$\begin{aligned} S(g_1+g_2+g_3) &= P(\lambda,\lambda) \;-\; 2 \\ &= 2C(\lambda,\lambda) \;+\; K(\lambda) \;-\; 2. \end{aligned}$$

Proof. The partial sum P is defined by (2.1). First, we reduce $S(g_1+g_2+g_3)$ to the simplified form as follows:

$$\begin{aligned} g_1+g_2+g_3 &= \lambda\left(\frac{v+1}{v^3}+\frac{v}{(v+1)^3}+\frac{1}{v}+\frac{1}{v+1}\right) \\ &= \lambda\left(\frac{1}{(v^2+v)^3}+\frac{1}{v^2+v}\right). \end{aligned}$$

Changing the variable $v^2+v=\xi$ with $Tr(\xi)=0$, we obtain

$$\begin{aligned} S(g_1+g_2+g_3) &= \sum_{v\in\mathbf{F}^{**}} e\left(\lambda\left(\frac{1}{(v^2+v)^3}+\frac{1}{v^2+v}\right)\right) \\ &= 2\sum_{\xi\in\mathbf{F}^{*}:\ Tr(\xi)=0} e\left(\lambda\left(\frac{1}{\xi^3}\;+\;\frac{1}{\xi}\right)\right) \\ &= 2\sum_{\zeta\in\mathbf{F}^{*}:\ Tr(1/\zeta)=0} e\left(\lambda(\zeta^3+\zeta)\right) \\ &= P(\lambda,\lambda) \;-\; 2. \end{aligned}$$

Here we have to explain why we return to summing over $\mathbf{F}^*$, but not $\mathbf{F}^{**}$ as we started. Indeed, $Tr(1)=0$, hence the equation $v^2+v=1$ always has a solution in $\mathbf{F}$, the field of order 2^m, for even m. Therefore, when we change v^2+v $(v\in\mathbf{F}^{**})$ to ξ we have to extend $\mathbf{F}^{**}$ into $\mathbf{F}^*$. Now using Lemma 11 we obtain the final expression. ∎

PROPOSITION 8. *Let $\lambda \neq 0$. Then*

$$\begin{aligned} S(g_1+g_2) &= P(\lambda,0) \;-\; 2 \\ &= C(\lambda) \;+\; G(\lambda,\lambda) \;-\; 2. \end{aligned}$$

Proof. We have

$$\begin{aligned} g_1+g_2 &= \lambda\left(\frac{v+1}{v^3}\;+\;\frac{v}{(v+1)^3}\right) \\ &= \lambda\left(\frac{1}{(v^2+v)^3}\right) \\ &= \frac{\lambda}{\xi^3} \;=\; \lambda\,\zeta^3, \end{aligned}$$

where we change variables $v^2 + v = \xi$ and then $1/\xi = \zeta$. Taking into account that $Tr(v^2 + v) = Tr(\xi) = Tr(1/\zeta) = 0$, we rewrite $S(g_1 + g_2)$ as follows:

$$\begin{aligned} S(g_1 + g_2) &= 2 \sum_{\zeta \in \mathbf{F}^*:\ Tr(1/\zeta)=0} e\,(\lambda \zeta^3) \\ &= P(\lambda, 0) \ - \ 2. \end{aligned}$$

Then we obtain the final expression using Lemma 12. □

PROPOSITION 9. *Let* $\lambda \neq 0$. *Then*

$$S(g_1 + g_3) \ = \ S(g_2 + g_3) \ = \ G(\lambda, \lambda) \ - \ 2.$$

Proof. Since $g_1(v) = g_2(v + 1)$ and $g_3(v) = g_3(v + 1)$ we deduce that $S(g_1 + g_3) = S(g_2 + g_3)$. So it is enough to compute $S(g_1 + g_3)$. First, we rewrite $g_1 + g_3$ as follows:

$$\begin{aligned} g_1 \ + \ g_3 &= \lambda \left(\frac{v+1}{v^3} \ + \ \frac{1}{v} + \frac{1}{v+1} \right) \\ &= \lambda \left(1 + \frac{v^2 + v + 1}{v^3} \ + \ 1 \ + \ \frac{1}{v+1} \right) \\ &= \lambda \left(\frac{(v+1)^3}{v^3} \ + \ \frac{v}{v+1} \right). \end{aligned}$$

Obviously, the mapping $v \mapsto (v + 1)/v$ is a 1-to-1 mapping from $\mathbf{F}^{**}$ onto $\mathbf{F}^{**}$. Therefore, changing $\xi = (v + 1)/v$, we obtain for $S(g_1 + g_3)$:

$$\begin{aligned} S(g_1 + g_3) &= \sum_{\xi \in \mathbf{F}^{**}} e \left(\lambda \left(\xi^3 \ + \ \frac{1}{\xi} \right) \right) \\ &= G(\lambda, \lambda) \ - \ 2. \end{aligned}$$ □

The proof of Theorem 1. Solving the system (4.5), we will, for short, use b and c during the proof instead of b' and c'.

We introduce two new variables

$$x \ + \ y \ = \ v, \quad xy \ = \ w.$$

As x, y, z, and u are all different, the element v belongs to the set $\mathbf{F}^{**}$. Using these new variables we can express $x^3 + y^3$ as follows:

$$x^3 \ + \ y^3 \ = \ v^3 \ + \ wv. \tag{4.6}$$

As $z + u = v + 1$ and $z^3 + u^3 = (v + 1)^3 + z\,u(v + 1)$ we can obtain from the second line of (4.5) that

$$w\,v \ + \ zu(v+1) \ = \ v^2 \ + \ v \ + \ b \ + \ 1. \tag{4.7}$$

Now we want, using the third line of (4.5), to obtain an expression similar to (4.7), which includes only new variables v and w and also the product $z\,u$. We have from (4.6) and the second line of (4.5)

$$\begin{aligned} (x+y)^5 &= x^5 \ + \ y^5 \ + \ xy(x^3 + y^3) \\ &= x^5 \ + \ y^5 \ + \ w(v^3 + w\,v) = v^5 \end{aligned}$$

and

$$\begin{aligned}(z+u)^5 &= z^5+u^5 \ + \ zu(z^3+u^3)\\ &= z^5 \ + \ u^5 \ + \ zu(x^3+y^3+b)\\ &= z^5 \ + \ u^5 \ + \ zu(v^3+wv+b) = (v+1)^5.\end{aligned}$$

Using these two expressions above and the third line of (4.5), we obtain

$$w^2\,v \ + \ w\,v^3 \ + \ zu\,(v^3+wv+b) \ = \ v^4 \ + \ v \ + \ c \ + \ 1. \tag{4.8}$$

We multiply (4.8) by $v+1$ and replace $z\,u$ by its value in (4.7), Thus, we get the following quadratic equation for w:

$$w^2v \ + \ w\,(v^2+v) \ + \ (v+1)(v^4+v+c+1) \ + \ (v^2+v+b+1)(v^3+b) \ = \ 0,$$

which gives, with $\lambda = c+1+b(b+1)$,

$$w^2 \ + \ w\,(v+1) \ + \ (v^2+v)(b+1)+b+c \ + \ \frac{\lambda}{v} \ = \ 0. \tag{4.9}$$

As we know from Lemma 2, this equation has two different roots in $\mathbf{F}$ if and only if

$$Tr\left(\frac{(v^2+v)(b+1)+b+c \ + \ \lambda/v}{(v+1)^2}\right) \ = \ 0. \tag{4.10}$$

Denote by $w_1 = w_1(v)$ and $w_2 = w_2(v)$ two distinct roots of (4.9). Now we return to the beginning of our proof. Two equalities $x \ + \ y \ = \ v$ and $x\,y \ = \ w_i$, $i \in \{1,2\}$, as well as two equalities $z+u = v+1$ and $z\,u = (w_i\,v+v^2+v+b+1)/(v+1)$ imply the two following trace conditions (Lemma 1):

$$Tr\left(\frac{w_i}{v^2}\right) \ = \ 0 \tag{4.11}$$

and

$$Tr\left(\frac{w_i\,v+v(v+1)+b+1}{(v+1)^3}\right) \ = \ Tr\left(\frac{w_i\,v+b+1}{(v+1)^3}\right) \ = \ 0. \tag{4.12}$$

As $w_1+w_2 = v+1$, it is easy to see that the validity of both conditions of (4.11) for one of w_i implies the validity of these conditions for the other.

Recall Lemma 14. Assume that (x,y,z,u) is a solution to (4.5) corresponding to $w_1 = w_1(v)$. Then it is easy to see that a 4-tuple $(x+1, y+1, z+1, u+1)$ is a solution to (4.5) corresponding to $w_2 = w_2(v)$.

Now we want to rewrite the conditions (4.11) and (4.12) in a more acceptable form. More exactly, using the fact that w_1 and w_2 are the roots of the quadratic equation (4.9), we want to eliminate w_i from the conditions (4.11) and (4.12). We

start from the first condition (let $w_i = w$):

$$\begin{aligned} Tr\left(\frac{w}{v^2}\right) &= Tr\left(\frac{w + wv + wv}{v^2}\right) = Tr\left(\frac{w(v+1)}{v^2} \ + \ \frac{w}{v}\right) \\ &= Tr\left(\frac{w(v+1) + w^2}{v^2}\right) \\ &= Tr\left(\frac{(v^2+v)(b+1) + b + c \ + \ \lambda/v}{v^2}\right) \\ &= Tr\left(b \ + \ \frac{b+1}{v} + \frac{b+c}{v^2} + \frac{\lambda}{v^3}\right) \\ &= Tr\left(b \ + \ \frac{(c+1) + b(b+1)}{v^2} + \frac{\lambda}{v^3}\right) \\ &= Tr\left(b \ + \ \lambda\left(\frac{v+1}{v^3}\right)\right), \end{aligned}$$

where we used the condition (4.9), that $Tr(x) = Tr(x^2)$ and $Tr(1) = 0$, since m is even. Thus (4.11) can be written as follows:

$$Tr\left(\lambda\left(\frac{v+1}{v^3}\right) \ + \ b\right) \ = \ 0. \tag{4.13}$$

Now we have for the condition (4.12):

$$\begin{aligned} Tr\left(\frac{wv + b + 1}{(v+1)^3}\right) &= Tr\left(\frac{wv + b + 1 + w + w}{(v+1)^3}\right) \\ &= Tr\left(\frac{w + b + 1}{(v+1)^3} + \frac{w}{(v+1)^2}\right) \\ &= Tr\left(\frac{w^2 + w(v+1) + (v+1)(b+1)}{(v+1)^4}\right) \\ &= Tr\left(\frac{(v+1)(b+1) + (v^2+v)(b+1) + b + c + \lambda/v}{(v+1)^4}\right) \\ &= Tr\left(\frac{\lambda}{v(v^4+1)} + \frac{(b+1)(v^2+1) + b + c}{v^4+1}\right) \\ &= Tr\left(\frac{\lambda}{v(v^4+1)} + \frac{b+1}{v^2+1} + \frac{b+c}{v^4+1}\right) \\ &= Tr\left(\frac{\lambda}{v(v^4+1)} + \frac{\lambda}{v^4+1}\right) = Tr\left(\frac{\lambda}{v(v+1)^3}\right). \end{aligned}$$

But

$$\frac{1}{v(v+1)^3} = \frac{1}{v} + \frac{1}{v+1} + \frac{1}{(v+1)^2} + \frac{1}{(v+1)^3}.$$

Hence we can rewrite the condition (4.12) as follows:

$$Tr\left(\lambda\left(\frac{v}{(v+1)^3} \ + \ \frac{1}{v} \ + \ \frac{1}{v+1}\right)\right) \ = \ 0. \tag{4.14}$$

Now we rewrite the condition (4.10). We have

$$\begin{aligned} & Tr\left(\frac{(v^2+v)(b+1)+b+c\ +\ \lambda/v}{(v+1)^2}\right) \\ &= Tr\left(b+\frac{b+1}{v+1}+\frac{b+c}{(v+1)^2}+\frac{\lambda}{v(v+1)^2}\right) \\ &= Tr\left(b+\frac{\lambda}{(v+1)^2}+\frac{\lambda}{v(v+1)^2}\right), \end{aligned}$$

using $v^2+v=v^2+1+v+1$ and properties of the trace function.

Thus the condition (4.10) is equivalent to the following condition:

$$Tr\left(b\ +\ \lambda\left(\frac{1}{v}\ +\ \frac{1}{v+1}\right)\right)=0. \tag{4.15}$$

We continue the proof of the theorem. So, in order to find the number $\mu(1,b,c)=\mu(\epsilon,\lambda)$ we have to find the following number, which we denote by $M(\epsilon,\lambda)$: *how many times all three conditions* (4.13), (4.14), *and* (4.15) *are simultaneously satisfied when* v *runs over* $\mathbf{F}^{**}$. It is easy to write the expression for the number $M(\epsilon,\lambda)$ in terms of exponential sums. Denote that (recall that $\lambda=\eta+1=b(b+1)+c+1$)

$$\begin{aligned} f_1 &= \lambda\left(\frac{v+1}{v^3}\right)\ +\ b, \\ f_2 &= \lambda\left(\frac{v}{(v+1)^3}\ +\ \frac{1}{v}\ +\ \frac{1}{v+1}\right), \\ f_3 &= \lambda\left(\frac{1}{v}\ +\ \frac{1}{v+1}\right)\ +\ b. \end{aligned}$$

By the definition we have

$$M(\epsilon,\lambda)=\frac{1}{8}\sum_{v\in\mathbf{F}^{**}}\left(1+(-1)^{Tr(f_1)}\right)\left(1+(-1)^{Tr(f_2)}\right)\left(1+(-1)^{Tr(f_3)}\right).$$

Multiplying into the parentheses and using our notation $e(a)=(-1)^{Tr(a)}$ and $\epsilon=Tr(b)$, we obtain

$$\begin{aligned} 8\,M(\epsilon,\lambda) = & \sum_{v\in\mathbf{F}^{**}}1+\sum_{v\in\mathbf{F}^{**}}e(f_1)+\sum_{v\in\mathbf{F}^{**}}e(f_2) \\ & +\sum_{v\in\mathbf{F}^{**}}e(f_3)+\sum_{v\in\mathbf{F}^{**}}e(f_1+f_2)+\sum_{v\in\mathbf{F}^{**}}e(f_1+f_3) \\ & +\sum_{v\in\mathbf{F}^{**}}e(f_2+f_3)+\sum_{v\in\mathbf{F}^{**}}e(f_1+f_2+f_3). \end{aligned}$$

Recall that $S(g)$ denotes the following exponential sum of g:

$$S(g)\ =\ \sum_{v\in\mathbf{F}^{**}}e(g(v)).$$

Introducing the following notation:

$$\begin{aligned} S_i &= S(f_i),\quad i=1,2,3, \\ S_{i,j} &= S(f_i+f_j),\quad i\neq j,\ i,j\in\{1,2,3\}, \\ S_{1,2,3} &= S(f_1+f_2+f_3), \end{aligned}$$

we obtain for the number $M(\epsilon, \eta)$,

$$8\,M(\epsilon,\lambda) = 2^m - 2 + S_1 + S_2 + S_3 + S_{1,2} + S_{1,3} + S_{2,3} + S_{1,2,3}.$$

Using the three functions $g_i(v)$, $i = 1, 2, 3$, introduced previously, and the fact that $g_2(v) = g_1(v+1)$, our separate sums can be written as follows:

$$\begin{aligned} S_1 &= S(g_1(v) + b), \\ S_2 &= S(g_2(v) + g_3(v)), \\ S_3 &= S(g_3(v) + b), \\ S_{1,2} &= S(g_1(v) + g_2(v) + g_3(v) + b), \\ S_{1,3} &= S(g_1(v) + g_3(v)), \\ S_{2,3} &= S(g_2(v) + b), \\ S_{1,2,3} &= S(g_1(v) + g_2(v)). \end{aligned}$$

Since $S(g + b) = -S(g)$ for the case $\epsilon = Tr(b) = 1$ and $S(g + b) = S(g)$ for the case $\epsilon = Tr(b) = 0$, we arrive at the following expression for the number $M(\epsilon, \lambda)$:

$$\begin{aligned} 8\,M(\epsilon,\lambda) &= 2^m - 2 + S(g_1 + g_2) + S(g_1 + g_3) + S(g_2 + g_3) \\ &\quad + (-1)^{\epsilon}\left(S(g_1) + S(g_2) + S(g_3) + S(g_1 + g_2 + g_3)\right). \end{aligned} \tag{4.16}$$

Using Propositions 5–9 for all of the sums in (4.16), and recalling our initial notation

$$\lambda = b'(b'+1) + c' + 1 = \frac{b}{a^3}\left(\frac{b}{a^3} + 1\right) + \frac{c}{a^5} + 1 = \eta + 1,$$

we obtain the expression for $M(\epsilon, \lambda)$ in the theorem for the case of even m. It remains to prove (4.2). When we introduce the new variables $v = x + y$ and $w = xy$, we could choose x and y in 6 different ways from the four variables x, y, z, u. But it is easy to see that two "opposite" choices of the new variables: $v = x+y$, $w = xy$, and $v = z+u$, $w = zu$ result in the same quadratic equation (4.9) for w. Of course it is possible to say the same about choices $v = x + z$, $w = x\,z$ and $v = y + u$, $w = y\,u$ (respectively, $v = x + u$, $w = x\,u$, and $v = y + z$, $w = y\,z$).

This means that for each proper value of $v \in \mathbf{F}^{**}$ (when all three trace conditions (4.10), (4.13), and (4.14) are satisfied), we obtain a solution $\{x, y, z, u\}$ as well as a solution $\{z, u, x, y\}$ (note that here any solution $\{x, y, z, u\}$ we consider is up to permutations between x and y and between z and u). Therefore, when v runs over $\mathbf{F}^{**}$ each solution $\{x, y, z, u\}$ occurs exactly three times. In other words, three distinct proper values of v result in the same solutions, namely $\{x, y, z, u\}$, $\{x, z, y, u\}$, and $\{x, u, y, z\}$. This means that

$$\mu(\epsilon,\lambda) \;=\; \frac{1}{3}\,M(\epsilon,\lambda),$$

i.e., we obtain the equality (4.2). The integer $M(\epsilon, \lambda)$ is even according to Lemma 14.

Now consider the case where $\lambda = 0$ or $c + 1 = b^2 + b$ (we again use the short notation b and c instead of b' and c'). For this case the trace conditions (4.13), (4.14), and (4.15) reduce, respectively, to

$$Tr(b) = 0,\ Tr(0) = 0, \quad \text{and} \quad Tr(b) = 0.$$

TABLE 1
$m = 6;\ p(x) = x^6 + x + 1.$

λ	$Tr(\lambda)$	C	C_0	K	G	$\mu(0,\lambda)$	$\mu(1,\lambda)$
1	0	0	16	− 8	0	2	4
α	0	8	− 8	0	− 8	2	0
α^3	0	0	16	− 8	0	2	4
α^5	1	8	− 8	12	0	4	0
α^7	0	8	− 8	0	8	4	2
α^9	0	16	16	8	0	6	0
α^{11}	1	− 8	− 8	− 4	16	2	6
α^{13}	0	− 8	− 8	8	− 8	0	2
α^{15}	1	0	16	4	− 8	2	2
α^{21}	1	− 16	16	12	8	2	6
α^{23}	1	8	− 8	− 12	0	2	2
α^{27}	0	0	16	16	16	6	4
α^{31}	1	− 8	− 8	− 4	0	0	4

Therefore, for the case $\epsilon = Tr(b) = 1$ our system (4.5) has no solutions, i.e., $\mu(1,0) = 0$. We proceed now with the case $\epsilon = Tr(b) = 0$. According to Lemma 13 (with $a = 1$), we have

$$\mu(1,b,c) = \mu(1,0,c+b^2+b) = \mu(1,0,1),$$

since $b^2 + b = c + 1$. Now consider the system (4.5) with $b = 0$ and $c = 1$. It is easy to check that $\{\beta, \beta^2, 0, 0\}$, where $\beta \in \mathbf{F}_4$ is of order 3, is a solution of (4.5). We deduce that the coset of syndrome $(a,b,c) = (1,0,1)$ has minimum weight 2 and then cannot contain any codeword of weight 4, *i.e., there is no solution of* (4.5) *composed of* 4 *pairwise distinct elements of* $\mathbf{F}$. This completes the proof of Theorem 1. □

As a direct corollary of Theorem 1, we obtain the following lower and upper bounds for the number $\mu(a,b,c)$, *i.e., the number of coset leaders in any coset* D *of weight* 4 *with syndrome* (a,b,c) *with* $a \neq 0$. We use the bounds for the exponential sums $K(\lambda)$, $G(\lambda,\lambda)$ and $C(\lambda)$, $C(\lambda,\lambda)$, involved in the number of solutions $\mu(a,b,c)$ (see Lemma 6, (2.4), and (2.5)).

THEOREM 2. *Let* a,b,c $(a \neq 0)$ *be any elements of* $\mathbf{F}$ *where* $\mathbf{F}$ *is the finite field of order* 2^m*, with* m *even and* $m \geq 10$. *Let* λ *be defined as in* (4.1). *If* λ *is a cube, then*

$$2^m - 8 - 26\sqrt{2^m} \leq 24\,\mu(a,b,c) \leq 2^m + 26\sqrt{2^m}.$$

If further $T_2^m((\lambda)^{2/3}) \neq 0$*, then*

$$2^m - 8 - 18\sqrt{2^m} \leq 24\,\mu(a,b,c) \leq 2^m + 18\sqrt{2^m}.$$

If λ *is not a cube, then*

$$2^m - 8 - 21\sqrt{2^m} \leq 24\,\mu(a,b,c) \leq 2^m + 21\sqrt{2^m}.$$

We note that the second bound is better than the corresponding bounds for odd m, obtained in [4] and [8].

TABLE 2
$m = 8;\ p(x) = x^8 + x^7 + x^6 + x + 1.$

λ	$Tr(\lambda)$	C	C_0	K	G	$\mu(0,\lambda)$	$\mu(1,\lambda)$
1	0	− 32	− 32	32	32	10	16
α	0	16	16	− 16	− 16	10	8
α^3	0	0	− 32	− 8	32	12	14
α^5	1	16	16	20	8	16	8
α^7	0	16	16	8	− 16	12	6
α^9	1	0	− 32	28	− 8	10	6
α^{11}	1	16	16	− 28	8	12	12
α^{13}	0	− 16	16	0	0	8	14
α^{15}	1	0	− 32	4	− 24	6	6
α^{17}	0	16	16	32	− 16	14	4
α^{19}	0	16	16	8	16	16	10
α^{21}	1	− 32	− 32	− 4	8	4	16
α^{23}	0	− 16	16	− 24	16	8	18
α^{25}	0	16	16	− 16	16	14	12
α^{27}	0	0	− 32	16	− 16	8	6
α^{29}	1	16	16	− 4	− 8	12	8
α^{31}	0	− 16	16	0	0	8	14
α^{37}	0	− 16	16	24	0	10	12
α^{39}	1	32	− 32	− 12	− 8	12	4
α^{43}	1	16	16	20	− 8	14	6
α^{45}	0	0	− 32	16	16	12	10
α^{47}	1	− 16	16	12	8	10	14
α^{51}	0	32	− 32	24	16	18	4
α^{53}	1	16	16	− 4	24	16	12
α^{55}	1	16	16	− 4	8	14	10
α^{59}	0	− 16	16	− 24	0	6	16
α^{61}	1	− 16	16	− 12	− 40	2	10
α^{63}	1	0	− 32	4	8	10	10
α^{85}	0	16	16	− 16	48	18	16
α^{87}	1	0	− 32	− 20	− 8	6	10
α^{91}	1	− 16	16	− 12	8	8	16
α^{95}	1	− 16	16	12	− 8	8	12
α^{111}	0	0	− 32	− 8	0	8	10
α^{119}	0	16	16	8	32	18	12
α^{127}	0	− 16	16	24	− 16	8	10

5. Numerical results. We present in Tables 1 and 2 the values of all exponential sums involved in the expression of $\mu(a, b, c)$ for $m = 6$ and $m = 8$. In Tables 1 and 2, the results are given for a set of representatives of the cyclotomic cosets only (since it is the same for all elements from such coset). We distinguish for a given λ two cases: $\epsilon = 0$ or $\epsilon = 1$ (with notation of Theorem 1). So for each value λ we give two numbers $\mu(1, \lambda)$ and $\mu(0, \lambda)$. For short, we use the following notation: $K = K(\lambda)$, $C = C(\lambda, \lambda)$, $C_0 = C(\lambda, 0)$, and $G = G(\lambda, \lambda)$. We denote by $p(x)$ the primitive

polynomial generating $\mathbf{F}$.

6. Conclusion. In this paper, we extended to the even case our work [4] on the coset leaders of cosets of weight 4 of the codes $BCH(2^m, 8)$. By Theorem 1 we summarized our results for both cases, m even and m odd. Recall that we gave in [6] the coset distribution of all codes $BCH(2^m, 8)$.

Now, the main open problem remains the computation of the weight distribution of all cosets. It has be shown for odd m that all is known as soon as the numbers $\mu(\epsilon, \lambda)$, and the number of times they occur, are known [3]. We conjecture that this property holds for even m. We introduced lower and upper bounds for the number of coset leaders of cosets of weight 4. We conjectured in [3] that this number takes all values between its bounds, up to some divisibility property. This conjecture was disproved in [8]. So the first question is: Which values are suitable?

New properties of exponential sums K, G, and C arise from formula (4.3) and (4.4) and from elements of their proofs. We developed this aspect in the odd case [5]. In the even case, the relations between K and C are more interesting since the spectrum of C is more complicated. We will study this fact in a forthcoming paper.

REFERENCES

[1] E. R. Berlekamp, H. Rumsey, and G. Solomon, *On the solution of algebraic equations over finite fields*, Information and Control, 12 (1967) pp. 553–564.
[2] L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand., 44 (1979), pp. 5–16.
[3] P. Charpin and V. A. Zinoviev, *On coset weight distributions of the* 3*-error-correcting BCH-codes*, SIAM J. Discrete Math., 10 (1997), pp. 128–145.
[4] P. Charpin, T. Helleseth, and V. A. Zinoviev, *On the cosets of weight* 4 *of binary BCH codes with minimum distance* 8 *and exponential sums*, Probl. Inf. Transm., 41 (2005), pp. 331–348.
[5] P. Charpin, T. Helleseth, and V. A. Zinoviev, *The divisibility modulo* 24 *of Kloosterman sums on* $GF(2^m)$*,* m *odd*, J. Combin. Theory Ser. A, 114 (2007), pp. 322–338.
[6] P. Charpin, T. Helleseth, and V. A. Zinoviev, *The coset distribution of triple-error-correcting binary primitive BCH codes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 1727–1732.
[7] P. Charpin, T. Helleseth, and V. A. Zinoviev, *Propagation characteristics of* $x \mapsto x^{-1}$ *and Kloosterman sums*, Finite Fields Appl., 13 (2007), pp. 366–381.
[8] G. van der Geer and M. van der Vlugt, *The coset weight distributions of certain BCH codes and a family of curves*, Enseign. Math., 48 (2002), pp. 3–21.
[9] T. Helleseth, *All binary* 3*-error-correcting BCH codes of length* $2^m - 1$ *have covering radius* 5, IEEE Trans. Inform. Theory, 24 (1978), pp. 257–258.
[10] T. Helleseth and V. A. Zinoviev, *On* Z_4*-linear Goethals codes and Kloosterman sums*, Des. Codes Cryptogr., 17 (1999), pp. 269–288.
[11] T. Helleseth and V. A. Zinoviev, *On coset weight distributions of the* Z_4*-linear Goethals codes*, IEEE Trans. Inform. Theory, 47 (2001), pp. 1758–1772,
[12] T. Helleseth and V. A. Zinoviev, *On a new identity for Kloosterman sums and nonlinear system of equations over finite fields of characteristic* 2, Discrete Math., 274 (2004), pp. 109–124.
[13] P. V. Kumar, T. Helleseth, R. A. Calderbank, and R. A. Hammons, *Large families of quaternary sequences with low correlation*, IEEE Trans. Inform. Theory, 42 (1996), pp. 579–592.
[14] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36 (1990), pp. 686–692.
[15] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, MA, 1983.
[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1986.